



## **Avaya Solution & Interoperability Test Lab**

---

# **Configuring Avaya Aura™ for Survivable Remote With a Core Avaya Aura™ Session Manager 6.0, Avaya Aura™ Communication Manager Evolution Server 6.0 and Avaya one-X® Deskphone Edition for 9600 SIP IP Telephones - Issue 1.0**

## **Abstract**

These Application Notes present a sample configuration for a network consisting of an Avaya Aura™ for Survivable Remote Branch with a core Avaya Aura™ Session Manager 6.0 and Avaya Aura™ Communication Manager Evolution Server 6.0 and Avaya one-X™ Deskphone Edition for 9600 Series SIP IP Telephones. Avaya Aura™ for Survivable Remote supports survivable local call processing and SIP routing for a branch that has become isolated from a main location due to an outage resulting in a loss of communication with a main location

Testing was conducted at the Avaya Solution and Interoperability Test Lab.

*(This Page Intentionally Left Blank)*

## **TABLE OF CONTENTS**

<b><u>1. INTRODUCTION.....</u></b>	<b><u>5</u></b>
<b><u>2. EQUIPMENT AND SOFTWARE VALIDATED.....</u></b>	<b><u>7</u></b>
<b><u>3. VERIFY INSTALLATION OF AVAYA AURA™ FOR SURVIVABLE REMOTE.....</u></b>	<b><u>8</u></b>
3.1. Verify Virtual Machine Status .....	8
3.2. Activate Survivable Remote Session Manager .....	8
3.3. Initialize Trust & Assign a SIP Entity IP Address .....	9
<b><u>4. CONFIGURE AVAYA AURA™ FOR SURVIVABLE REMOTE.....</u></b>	<b><u>10</u></b>
4.1. Configure Survivable Remote Communication Manager .....	10
4.1.1. Configure Server Role .....	10
4.2. Configure G450 Media Gateway.....	12
4.2.1. Configure Media Gateway Controller List .....	12
4.2.2. Administer a Transition Point .....	13
4.2.3. Administer Search Timers.....	13
4.2.4. Verify Recovery Settings.....	13
4.2.5. Save Gateway Configuration .....	13
<b><u>5. CONFIGURE AVAYA AURA™ COMMUNICATION MANAGER.....</u></b>	<b><u>14</u></b>
5.1. Add Node Names for Survivable Remote Branch .....	14
5.2. Administer a Survivable Server for Survivable Remote Communication Manager .....	15
5.3. Add a Branch Media Gateway.....	16
5.4. Administer an IP Network Region for the Branch .....	17
5.5. Administer an IP Codec Set for Calls to/from the Branch .....	18
5.6. Administer IP Network Map for Branch IP Telephones .....	19
5.7. Update Dial Plan for the Branch Location .....	20
5.8. Update Private Numbering for Branch Location .....	20
5.9. Administer Stations for the Survivable Branch Location .....	21
5.10. Save Changes.....	21

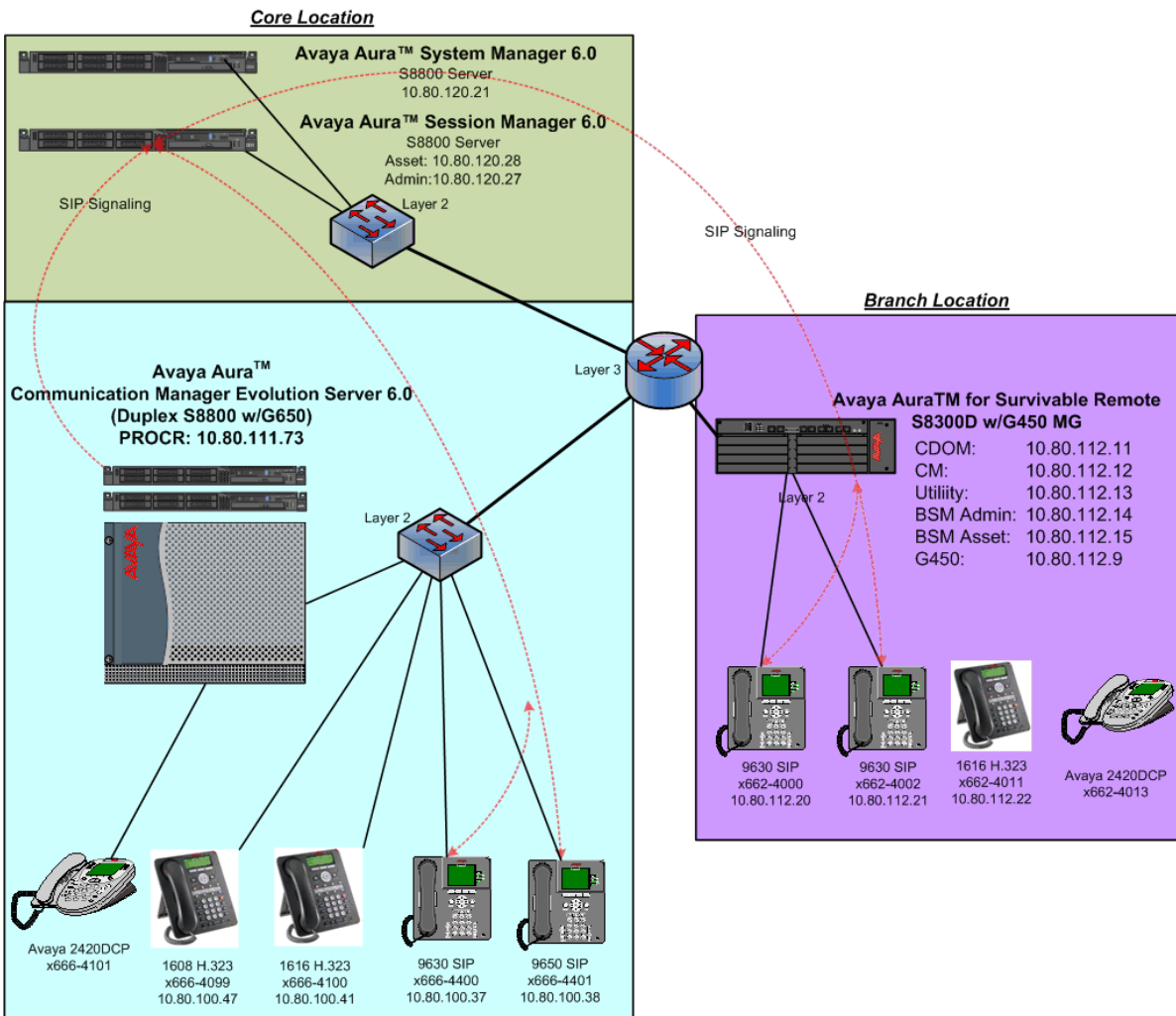
<b>6.</b>	<b><u>CONFIGURE AVAYA AURA™ SESSION MANAGER .....</u></b>	<b><u>22</u></b>
6.1.	Log in to Avaya Aura™ System Manager .....	22
6.2.	Define a Location for the Survivable Remote Branch .....	23
6.3.	Administer the Survivable Remote Session Manager as a SIP Entity.....	24
6.4.	Define Ports & Protocols for use by Survivable Remote Session Manager .....	25
6.5.	Administer Entity Links .....	26
6.6.	Define Survivable Remote Session Manager to System Manager .....	26
6.7.	Administer Routing Policies and Dial Pattern .....	27
6.8.	Administer SIP Users and Survivable Branch Stations .....	29
6.8.1.	Add a SIP User and Corresponding Station.....	29
6.8.2.	Add a non-SIP Station .....	34
6.9.	Synchronize Communication Manager with System Manager.....	38
<b>7.</b>	<b><u>CONFIGURE THE AVAYA 9600 SERIES SIP IP TELEPHONE.....</u></b>	<b><u>39</u></b>
7.1.	Configuration Using DHCP and 46xxsettings.txt.....	39
7.1.1.	DHCP Settings .....	39
7.1.2.	46xxsettings.txt Parameters .....	40
7.2.	Configure the Avaya one-X® Deskphone Edition for 9600 SIP IP Telephone Manually .....	41
7.2.1.	Configure IP Address, Subnet Mask & Default Gateway .....	41
7.2.2.	Configure SIP Global and Proxy Settings .....	43
7.2.3.	Log in Phone to Avaya Aura™ Session Manager.....	45
<b>8.</b>	<b><u>VERIFY INSTALLATION.....</u></b>	<b><u>46</u></b>
8.1.	Verify Avaya Aura™ Communication Manager Evolution Server .....	46
8.1.1.	Verify Survivable Server Status.....	46
8.1.2.	Verify Media Gateway Registration Status.....	46
8.2.	Verify Avaya Aura™ Session Manager.....	46
8.2.1.	Verify Database Replication Status.....	46
8.2.2.	Verify Status of 9600 Series SIP Telephones .....	47
<b>9.</b>	<b><u>SURVIVABILITY SCENARIOS .....</u></b>	<b><u>47</u></b>
<b>10.</b>	<b><u>CONCLUSION.....</u></b>	<b><u>48</u></b>
<b>11.</b>	<b><u>REFERENCES.....</u></b>	<b><u>48</u></b>

# 1. Introduction

For release 6.0, Avaya has introduced two new concepts with its Avaya Aura™ Communication Manager line of telephony servers:

- Avaya Aura™ Communication Manager Evolution Server which supports all Avaya-manufactured endpoints including H.323, DCP, analog and SIP.
- Avaya Aura™ for Survivable Remote which builds on the Local Survivable Processor (LSP) concept by adding a survivable Avaya Aura™ Session Manager to the S8300D and S8800 platforms, thus bringing SIP survivability to the branch location.

Avaya Aura™ for Survivable Remote supports survivable local call processing and SIP routing for a branch that has become isolated from a ‘core’ (or ‘main’) location due to an outage resulting in loss of communication with the core location. The purpose of these application notes is to describe the necessary steps to administer a Survivable Remote for connectivity and survivability with an Avaya Aura™ Session Manager and Communication Manager Evolution Server located at the ‘core’.



**Figure 1: Sample Configuration Topology**

The complete sample network is shown above in **Figure 1**, where Avaya Aura™ Session Manager routes all inter-system calls between the ‘core’ (or ‘main’) location and the branch location. However these Application Notes will only describe the necessary steps to add Avaya Aura™ for Survivable Remote to an already installed and configured ‘core’ Avaya Aura™ Session Manager and Communication Manager Evolution Server. See the reference documents in **Section 11** for additional information on installing configuring these platforms.

SIP trunks are used to interconnect these systems to Avaya Aura™ Session Manager. All inter-system calls are carried over these SIP trunks. Avaya Aura™ Session Manager can support flexible inter-system call routing based on dialed number, calling number and system location, and can also provide protocol adaptation to allow for multi-vendor systems to interoperate. Avaya Aura™ Session Manager is managed by a separate Avaya Aura™ System Manager, which can manage multiple Avaya Aura™ Session Managers.

**NOTE:** These application notes do not cover the necessary administration steps for a ‘ground up’ installation of any of the described components. This document is written from the

perspective that all the necessary hardware and software has already been installed. See **Section 11** for additional installation and reference documentation.

## 2. Equipment and Software Validated

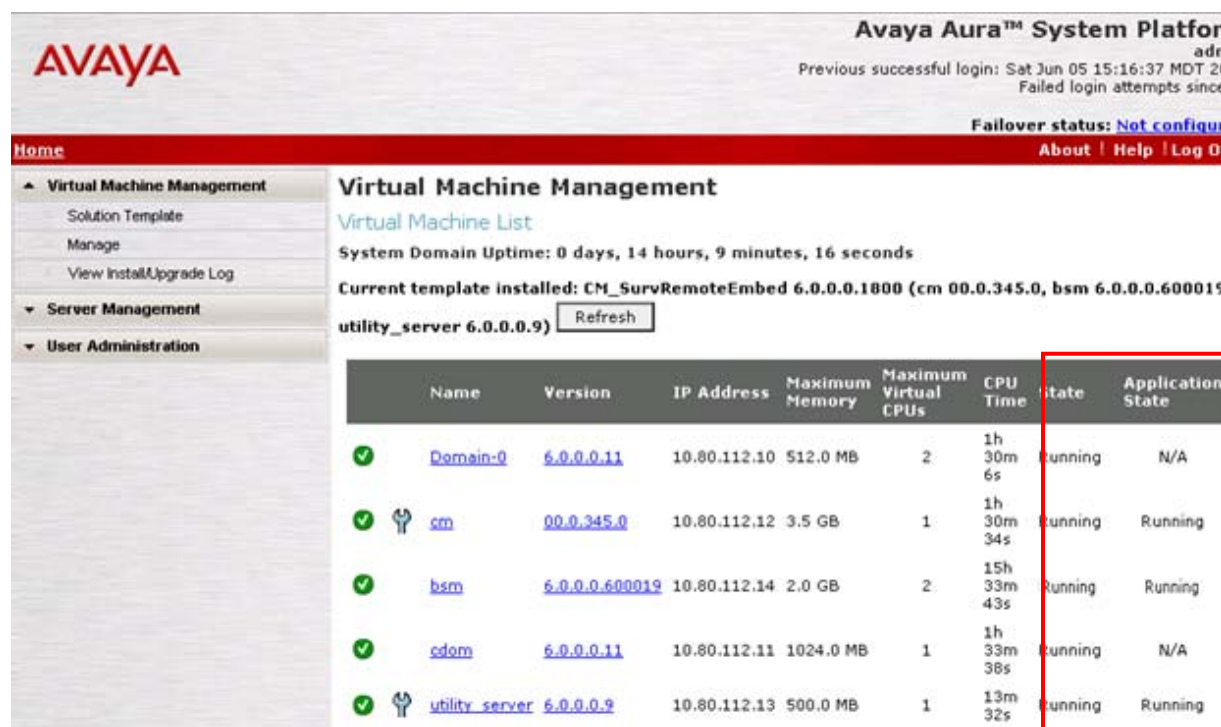
The following equipment and software/firmware were configured and verified for the sample configuration.

Hardware Component	Software/Firmware Version
Avaya S8800 Server	Avaya Aura <sup>TM</sup> Session Manager 6.0
Avaya S8800 Server	Avaya Aura <sup>TM</sup> System Manager 6.0
Avaya S8800 Server (duplex)	Avaya Aura <sup>TM</sup> Communication Manager Evolution Server 6.0
Avaya S8300D Server	Avaya Aura <sup>TM</sup> for Survivable Remote Embedded Version 6.0.
Avaya G450 Media Gateway	FW 30.12.1
Avaya 9630 one-X <sup>TM</sup> Deskphone (SIP)	2.6
Avaya 9630 one-X <sup>TM</sup> Deskphone (H.323)	3.0
Avaya 2420 DCP Telephone	6

## 3. Verify Installation of Avaya Aura™ for Survivable Remote

### 3.1. Verify Virtual Machine Status

Before configuring the Survivable Remote, it is recommended to check that the installation was successfully completed. To complete this step, open a web browser to the following URL: **Error! Hyperlink reference not valid.** and login with appropriate credentials. In the sample configuration this IP address is 10.80.112.11. Verify that the **cm**, **bsm** and **utility servers** **State** and **Application State** are **running** (as shown below).



Avaya Aura™ System Platform

Previous successful login: Sat Jun 05 15:16:37 MDT 2010  
Failed login attempts since: 0

Failover status: **Not configured**

Home About Help Log Out

**Virtual Machine Management**

Solution Template  
Manage  
View Install/Upgrade Log

**Server Management**

**User Administration**

**Virtual Machine Management**

Virtual Machine List

System Domain Uptime: 0 days, 14 hours, 9 minutes, 16 seconds

Current template installed: CM\_SurvRemoteEmbed 6.0.0.0.1800 (cm 00.0.0.345.0, bsm 6.0.0.0.600019, utility\_server 6.0.0.0.9)

Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
Domain-0	6.0.0.0.11	10.80.112.10	512.0 MB	2	1h 30m 6s	Running	N/A
cm	00.0.0.345.0	10.80.112.12	3.5 GB	1	1h 30m 34s	Running	Running
bsm	6.0.0.0.600019	10.80.112.14	2.0 GB	2	15h 33m 43s	Running	Running
cdom	6.0.0.0.11	10.80.112.11	1024.0 MB	1	1h 33m 38s	Running	N/A
utility_server	6.0.0.0.9	10.80.112.13	500.0 MB	1	13m 32s	Running	Running

### 3.2. Activate Survivable Remote Session Manager

It is possible that the Survivable Remote Session Manager was installed in an 'inactive' state. If this were the case the **bsm** Application State would show as **Stopped** unlike what is shown in **Section 3.1** above.

To activate the Survivable Remote Session Manager, have the following information available:

- DNS search string
- System Manager's IP address
- System Manager's Fully Qualified Domain Name (FQDN)
- Enrollment Password administered in System Manager

Next, SSH in to the CDOM on the S8300D server with the appropriate credentials (**do not use root**) and run the following command:

## /opt/vsp/activateBSM

The script prompts for the above information and will display a summary when complete. If the information displayed is incorrect hit <CTRL+c> to start over, otherwise hit <ENTER> to activate Session Manager, which will reboot Session Manager. Wait at least 10 minutes and log back in to the CDOM to verify the status of 'bsm' per **Section 3.1**.

NOTE: Once a Survivable Remote Session Manager has been activated it cannot be deactivated.

### 3.3. Initialize Trust & Assign a SIP Entity IP Address

Before the Survivable Remote Session Manager can be administered in System Manager two things must happen:

- 1) An IP address must be assigned to the SIP Entity interface.  
NOTE: For the S8300D server, this IP address must be in the same subnet as the administration interface configured during installation.
- 2) 'Trust' with System Manager must be initialized from the Survivable Remote Session Manager

Both of these items are administered on the same screen. To complete this admin have an additional IP address and the System Manager Enrollment Password ready. See the references in **Section 11** on how to set and/or obtain the enrollment password in System Manager.

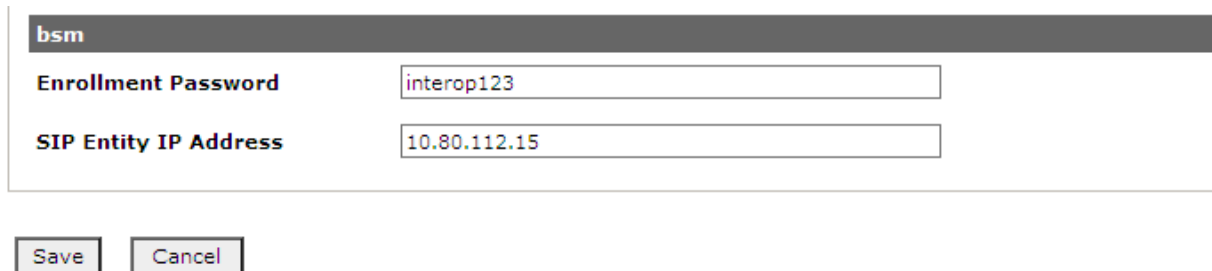
To set these values open a web browser to the following URL: **Error! Hyperlink reference not valid.** and login with appropriate credentials.

(In the sample configuration this IP address is 10.80.112.11.)

In the left pane expand **Server Management** and select **Network Configuration**. Scroll down to the bottom of screen that appears to the section titled **bsm** (as shown) and fill in the following entries:

- **Enrollment Password** Replace **SIP-NOT-USED** with the System Manager enrollment password.
- **SIP Entity IP Address:** Enter in a unique IP address.

Select **Save** when complete.



bsm	
Enrollment Password	interop123
SIP Entity IP Address	10.80.112.15

## 4. Configure Avaya Aura™ for Survivable Remote

### 4.1. Configure Survivable Remote Communication Manager

#### 4.1.1. Configure Server Role

From a web browser, login to the System Management Interface (SMI) using the following URL: **Error! Hyperlink reference not valid.** where CM-IP-Address is the IP address or hostname of the Survivable Remote Communication Manager. As shown in **Figure 1**, this IP is 10.80.112.12.

From the left-pane navigate to **Server Configuration** and select **Server Role** as shown below. For the sample configuration the following values were administered:

- **This server is:** Select the radio button '**a local survivable server (LSP)**
- **SID:** System ID. Should match the core Communication Manager's
- **MID:** Module ID. Will be a unique value to identify this branch
- **Registration address at the main server** IP address of a **CLAN** or the **Procr** interface on the core Communication Manager
- **File Synchronization address at the main cluster** IP address of the 'customer LAN' interface on the Communication Manager server(s) at the core location. Do not use the 'active' IP address.

AVAYA

Avaya Aura™ Communication Manager System Management Interface

[Help](#)
[Log Off](#)

[Administration](#)
[Upgrade](#)

Administration / Server (Maintenance)

This Server

Alarms

Current Alarms

Agent Status

SNMP Agents

SNMP Traps

Filters

SNMP Test

Diagnostics

Restarts

System Logs

Ping

Traceroute

Netstat

Server

Status Summary

Process Status

Shutdown Server

Server Date/Time

Software Version

Server Configuration

Server Role

Network Configuration

Static Routes

Display Configuration

Server Upgrades

Manage Updates

Data Backup/Restore

Backup Now

Backup History

Schedule Backup

Backup Logs

View/Restore Data

Restore History

Security

Administrator Accounts

Login Account Policy

Login Reports

Server Role

This page allows for the specification of the Server's Role.

WARNING:

- Changing the role of this server will **erase any translations** residing on this server and will cause a **Communication Manager reset**. If you wish to preserve existing translations, execute a backup prior to completing this page.
- A restart of Communication Manager is needed after the server has been successfully configured. Click the **Restart CM** button below to do so. Please note that this should be done after all configuration is completed. Too many restarts may escalate to a full Communication Manager reboot.
- This server appears to be the **ACTIVE** server. This server will be unavailable for telephony during the configuration process.

Server Settings

**This Server is:**

☒ a local survivable server (LSP)

**System ID and Module ID:**

SID:

MID:

Configure Survivable Data

Specify the interfaces on the main server(s) that this server will use for registration and file synchronization.

**IPv6 is currently disabled.**

Component	IPv4 Address	IPv6 Address
Registration address at the main server (CLAN or PE Address)	<input type="text" value="10.80.111.76"/>	<input type="text"/>
File Synchronization address at the main cluster (PE Address)	<div>Main Server <input type="text" value="10.80.111.72"/></div> <div>Duplicate Server* <input type="text" value="10.80.111.82"/></div>	<div>Main Server <input type="text"/></div> <div>Duplicate Server* <input type="text"/></div>

The following screenshot is the lower-half of the screen shown above:

- This Server's Memory Settings:**

'Large Survivable'

This should match the value shown directly below for **Main Server's Memory Settings**

File Synchronization address at the alternate\*\* main cluster (PE Address)

Main Server

Duplicate Server\*

Main Server

Duplicate Server\*

\* only if servers are duplicated

\*\* if used

Configure Memory

This Server's Memory Setting:

Main Server's Memory Setting: **Large**

Optional LSP Media Gateway Serial Number

If this LSP registers with a CM5.1.2 or earlier main server, you may need to enter the serial number of a media gateway in order to register with the main server. To obtain a media gateway serial number, execute the list media-gateway SAT command and select one of the media gateway serial numbers displayed.

Media Gateway Serial Number:

Change

Restart CM

Help

## 4.2. Configure G450 Media Gateway

### 4.2.1. Configure Media Gateway Controller List

In order to register with Communication Manager at the Core, the media-gateway needs to know what IP address(es) it can register to. Generally this can be either a C-LAN or Processor Ethernet (procr) interface. Additionally, the media-gateway must also know about any survivable processors it can register with. This list of IP addresses is called the **media-gateway controller (or mgc) list**.

To configure the **mgc list** SSH in to the G450 with the appropriate credentials and run the command **show mgc list**. The screenshot below shows there are already 3 entries on the G450.

```
G450-001(super)# show mgc list

CONFIGURED MGC HOST
-----
10.10.11.20
10.10.12.20
10.10.13.30
-- Not Available --
sls                               disabled
```

-Use the command **clear mgc list** to remove any existing entries.

-Use the command **set mgc list x.x.x.x, y.y.y.y** to enter one or more mgc IP addresses.

Multiple IP addresses (up to 4) can be entered as long as each one is separated by a comma. Additionally these should be listed in order of preference. In the sample configuration the G450 is configured with two addresses; the first is the **Procr** interface on the core Communication Manager instance and the second is the **Procr** interface on the Survivable Remote Communication Manager instance.

Below are the entries used in the sample configuration.

```
G450-001(super)# clear mgc list
Done!
G450-001(super)# set mgc list 10.80.111.76,10.80.112.12
Done!
G450-001(super)# show mgc list

CONFIGURED MGC HOST
-----
10.80.111.73
10.80.112.12
-- Not Available --
-- Not Available --
sls                               disabled

Done!
G450-001(super)#
```

### 4.2.2. Administer a Transition Point

A transition point represents a position in the **mgc-list** and is used to separate survivable MGC's from those that are available during normal operations. Also, once the Primary Search timer has expired without the media-gateway having successfully registered it will begin to include any IP addresses below this point in registration attempts. In the sample configuration there are only two MGC's in the list, with the second one being used for survivability. Therefore the transition point in the sample configuration is '1'. The command **set reset-times transition-point 1** is used to set this value.

### 4.2.3. Administer Search Timers

In order to maintain functionality during an outage scenario, there are two timers that must be administered on the media-gateway:

**Primary Search Timer:** This is the amount of time (in minutes) that the media-gateway will cycle through the **mgc-list**, up to and including the transition point, in its attempts to register.

**Total Search Timer:** Once the Primary Search Timer has expired the media-gateway will begin to include any IP addresses after the Transition Point in its attempts to register. It will cycle through all the IP addresses in the MGC list for the length of the **Total Search Timer** (in minutes). If the **Total Search Timer** expires without a successful registration, the media-gateway will reset and the process will begin anew.

The commands to configure these timers are **set reset-times primary-search x** and **set reset-times total-search y**, where 'x' is a value of 1-59 [minutes] and 'y' is a value of 2-60 [minutes]. The sample configuration settings are shown in the next section.

### 4.2.4. Verify Recovery Settings

To verify the media-gateway recovery settings, run the command **show recovery**. The screenshot below shows the information configured in the previous two steps:

```
G450-001(super)# show recovery

RECOVERY TIMES
-----
Primary Search   : 1
Total Search     : 2
Transition Point : 1
```

### 4.2.5. Save Gateway Configuration

Once the changes to the G450 are complete, run the command **copy running-config startup-config** to save the changes.

```
G450-001(super)# copy running-config startup-config
Warning! It is a recommended policy to override default configuration
master key with user defined secret - for details see user reference.
Otherwise device saves configuration secrets using Avaya default secret.
Beginning copy operation ..... Done!
```

## 5. Configure Avaya Aura™ Communication Manager Evolution Server

This section shows only the necessary configuration in Communication Manager to add the Survivable Remote Branch configuration. This section includes the following configuration steps:

- Add node-names for Survivable Remote branch
- Administer a survivable-server for Survivable Remote branch
- Add branch media-gateway
- Administer ip-network-region for the branch location
- Administer an ip-codec-set for calls to/from the branch location
- Administer dial plan parameters for extensions at the branch location
- Administer private-numbering for extensions at the branch location
- Add a station for the Survivable Remote branch
- Save Changes

### 5.1. Add Node Names for Survivable Remote Branch

The first step in administering a Survivable Remote Branch on the core Communication Manager is to add node-names for the survivable Session Manager and Communication Manager instances. To do so login to the System Access Terminal (SAT) interface on the core Communication Manager and run the command **change node-names ip**. For the sample configuration the following values were administered:

- **BSM-LSP1** '10.80.112.12'. This is the IP address of processor ethernet (procr) interface on the S8300D
- **BSM1-SM1** '10.80.112.15'. This is the IP address of Asset interface on the Survivable Remote Session Manager

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
ASM1-SM100	10.80.120.28	
ASM2-SM100	10.80.120.30	
<b>BSM-LSP1</b>	<b>10.80.112.12</b>	
<b>BSM1-SM1</b>	<b>10.80.112.15</b>	
IPOR6	33.1.1.104	
MgmtPC1	10.80.51.40	
VAL01a08	10.80.111.90	
clan-1a04	10.80.111.76	
default	0.0.0.0	
gateway1	10.80.111.1	
procr	10.80.111.73	
procr6	::	
xfire-1a02	10.80.111.77	

## 5.2. Administer a Survivable Server for Survivable Remote Communication Manager

Next, add a survivable-server using the command **add survivable-processor xxxx** where 'xxxx' is the **node-name** of processor ethernet (**procr**) interface on the S8300D and administered in the previous section. For the sample configuration the following values were administered:

- **Node-name** 'BSM-LSP1'
- **Type** 'lsp'. For Local Survivable Processors
- **Cluster ID/MID** '2'. Should match the value used in **Section 4.1.1**
- **Processor Ethernet Network Region** '3'. The ip-network-region used to represent the branch location.

```
add survivable-processor BSM-LSP1                                     Page 1 of 1
                                SURVIVABLE PROCESSOR

Type: lsp                  Cluster ID/MID: 2    Processor Ethernet Network Region: 3

V4 Node Name: BSM-LSP1      Address: 10.80.112.12
V6 Node Name:               Address:
```

### 5.3. Add a Branch Media Gateway

The sample configuration shows a G450 media gateway at the branch location. During normal operation this gateway is *controlled by* and *registered to* the Communication Manager instance at the core location.

To add a G450 media-gateway to Communication Manager use the command **add media-gateway x** where 'x' is a number from 1-250. For the sample configuration the following values were administered:

- **Type** 'g450'. Choose the appropriate type for the media-gateway hardware
- **Name** 'G450 BSM1'. A descriptive name for the media-gateway
- **Serial No** This is the serial number for the media-gateway. See **Section 11** on how to obtain the gateway's serial number.
- **Encrypt Link?** 'n'. Choose 'y' or 'n' to encrypt the signaling between Communication Manager and the media-gateway

The remaining fields are filled in automatically when the gateway has successfully registered to Communication Manager.

```
add media-gateway 1                                     Page 1 of 2
                                     MEDIA GATEWAY 1
                                     Type: g450
                                     Name: G450 BSM1
                                     Serial No: 08IS35197397
                                     Encrypt Link? n
                                     Network Region: 3
                                     Location: 1
                                     Site Data:
                                     Recovery Rule:
                                     Registered? n
                                     FW Version/HW Vintage:
                                     MGP IPV4 Address:
                                     MGP IPV6 Address:
                                     Controller IP Address:
                                     MAC Address:
```

## 5.4. Administer an IP Network Region for the Branch

In the sample configuration, the branch location was configured to be in ip-network-region 3 while the core location is in ip-network-region 1. In order to complete calls between the two locations its necessary connect the two regions together.

Using the **change ip-network-region 3** command set the **Authoritative Domain** to the correct SIP domain for the configuration. Verify the **Intra-region IP-IP Direct Audio**, and **Inter-region IP-IP Direct Audio** fields are set to “yes”.

```
change ip-network-region 3                                     Page 1 of 19
                                                                IP NETWORK REGION
Region: 3
Location: 1      Authoritative Domain: avaya.com
Name: Branch 1
MEDIA PARAMETERS
Codec Set: 1      Intra-region IP-IP Direct Audio: yes
                  Inter-region IP-IP Direct Audio: yes
UDP Port Min: 2048      IP Audio Hairpinning? n
UDP Port Max: 16585
```

Navigate to **page 3** and add the node-name for the Survivable Remote Communication Manager to the **Backup Servers** list.

```
change ip-network-region 3                                     Page 3 of 20
                                                                IP NETWORK REGION

INTER-GATEWAY ALTERNATE ROUTING / DIAL PLAN TRANSPARENCY
Incoming LDN Extension:
Conversion To Full Public Number - Delete:      Insert:
Maximum Number of Trunks to Use for IGAR:
Dial Plan Transparency in Survivable Mode? n

BACKUP SERVERS(IN PRIORITY ORDER)      H.323 SECURITY PROFILES
1      BSM-LSP1                          1      challenge
2                                  2
3                                  3
4                                  4
```

Navigate to **page 4** and administer ip-network-region 1 and 3 to be directly connected to each other by adding a ‘y’ under the **direct WAN** column and to use **ip-codec-set 3** as shown.

```
change ip-network-region 3                                     Page 4 of 20

Source Region: 3      Inter Network Region Connection Management
dst codec direct      WAN-BW-limits      Video      Intervening      Dyn      G      A      M
rgn set  WAN  Units      Total Norm      Prio Shr      Regions      CAC      R      L      e
1      3      y      NoLimit                                n      t
2                                  n      t
3      1                                all
```

## 5.5. Administer an IP Codec Set for Calls to/from the Branch

In the sample configuration, calls that are between the two regions should use the G.729A codec to conserve bandwidth utilization. To configure this it is necessary to administer the ip-codec-set referenced in **Section 5.4** using the command '**change ip-codec-set 3**'. Administer **G.729A** as the first codec and **G.711MU** as a secondary codec (optional).

change ip-codec-set 3

Page1 of 2

IP Codec Set

Codec Set: 3

	Audio	Silence	Frames	Packet
	Codec	Suppression	Per Pkt	Size(ms)
1:	<b>G.729A</b>	n	2	20
2:	<b>G.711MU</b>	n	2	20
3:				
4:				
5:				
6:				
7:				

Media Encryption

1: none

2:

## 5.6. Administer IP Network Map for Branch IP Telephones

In the sample configuration, the branch location is considered to be in ip-network-region 3, therefore IP phones at that location will belong to ip-network-region 3 as well. Use the command **change ip-network-map** to assign the phones at this location to the region via their IP address. For the sample configuration phones in the subnet 10.80.112.0/24 will be placed in ip-network-region 3.

- **FROM:** '10.80.112.0' Enter in an IP address or subnetwork address
- **Subnet Bits:** '24' The number of bits in the subnet mask
- **Network Region:** '3' Enter the desired **ip-network-region** value
- **TO:** This is filled in automatically if **Subnet Bits** is populated. Otherwise enter in an IP address to represent the end of the range of IP addresses

change ip-network-map

63

Page 1 of

IP ADDRESS MAPPING

IP Address	Subnet	Network	Emergency
Ext	Bits	Region	VLAN Location
-----			
---			
FROM: 10.80.60.224	/27	2	n
TO: 10.80.60.255			
FROM: 10.80.61.32	/27	7	n
TO: 10.80.61.63			
FROM: 10.80.100.0	/24	2	n
TO: 10.80.100.255			
<b>FROM: 10.80.112.0</b>	<b>/24</b>	<b>3</b>	<b>n</b>
<b>TO: 10.80.112.255</b>			

## 5.7. Update Dial Plan for the Branch Location

For the sample configuration extensions at the branch location use a different digit string (662xxxx) than those at the core location (666xxxx), therefore it's necessary to add this digit string to Communication Manager's dial plan. Use the command **change dialplan analysis** to add the digit string 662xxxx.

- **Dialed String**    **'662'** Digit pattern for the new extension range
- **Total Length**    **'7'** Total number of digits in an extension
- **Call Type**        **'ext'** Indicates this range is for local extensions

change dialplan analysis									Page 1 of 12
DIAL PLAN ANALYSIS TABLE									
Location: all									Percent Full: 2
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	
0	1	attd							
1	2	dac							
2	2	fac							
3	6	aar							
<b>662</b>	<b>7</b>	<b>ext</b>							
6661	7	ext							
6668	7	ext							

## 5.8. Update Private Numbering for Branch Location

Generally, SIP Users registered to Session Manager need to be added to either the private or public numbering table on the Communication Manager Evolution Server. For the sample configuration, **private** numbering was used and all extension numbers were unique within the private network.

In the sample configuration, the private numbering table needs to be updated to accommodate the newly added extension range **662xxxx**. Use the command "**change private-numbering 7**" to define the caller ID number which will be sent out with these calls over trunk-group 10.

- **Ext Len:** Enter the extension length allowed by the dial plan
- **Ext Code:** Enter leading digit (s) from extension number
- **Trunk Grp:** Enter the SIP Trunk Group number for the SIP trunk between the Evolution Server and Session Manager
- **Private Prefix:** Leave blank unless an enterprise canonical numbering scheme is defined in Session Manager. If so, enter the appropriate prefix

change private-numbering 7					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext Len	Ext Code	Trk Grp(s)	Private Prefix	Total Len	
<b>7</b>	<b>662</b>	<b>10</b>		<b>7</b>	Total Administered: 2
7	666	10		7	Maximum Entries: 540

## 5.9. Administer Stations for the Survivable Branch Location

While it is possible to administer stations directly on Communication Manager, it is recommended that station administration be performed using Avaya Aura™ System Manager. See the references in **Section 11** for more information on how to setup and administer Communication Manager in System Manager for administration. See **Section 6.8** on how to administer SIP users and stations via System Manager.

## 5.10. Save Changes

Use the **save translation** command to save all changes.

save translation	
SAVE TRANSLATION	
Command Completion Status	Error Code
Success	0

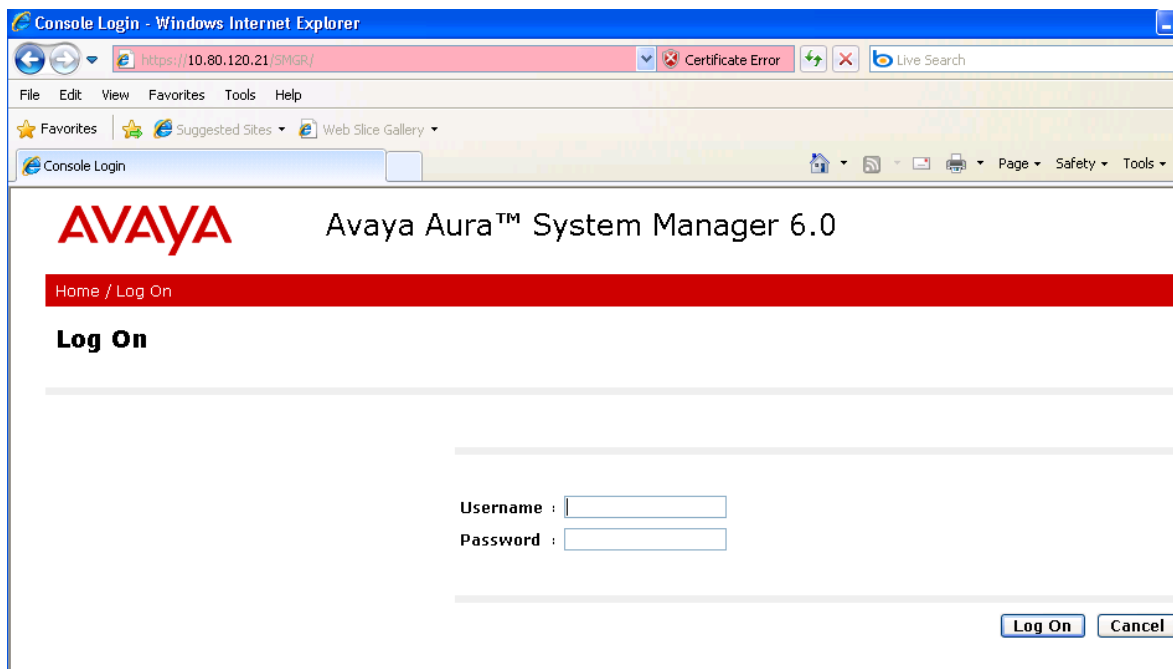
## 6. Configure Avaya Aura™ Session Manager

This section provides the procedures for adding the Avaya Aura™ for Survivable Remote Session Manager as a SIP Element to the core Session Manager. For further information on configuring Session Manager, please see additional reference documentation listed in **Section 11**. This section includes the following admin and configuration steps:

- Log in to Avaya Aura™ System Manager
- Define a location for the Survivable Remote branch
- Administer the Survivable Remote as a SIP Entity
- Administer Entity Links
- Administer Dial Patterns
- Administer SIP users and Survivable Branch stations

### 6.1. Log in to Avaya Aura™ System Manager

Access the Avaya Aura™ System Manager using a Web Browser and entering <http://<ip-address>/SMGR>, where <ip-address> is the IP address of System Manager. Log in using the appropriate credentials and accept the subsequent Copyright Legal Notice.



## 6.2. Define a Location for the Survivable Remote Branch

Locations can be defined in Session Manager to assist with call routing as well as to measure, monitor and limit bandwidth usage amongst the different locations. This is an optional but recommended parameter to configure. Locations are defined by an IP address or address pattern. The Locations screen can contain one or several IP addresses. Each SIP entity has a particular IP address. Depending on the physical and geographic location of each SIP entity, some of the SIP Entities can be grouped into a single location. For example, if there are two Communication Managers located at Denver, they can form one location named 'Denver'.

To add a location for the branch, in the left-pane of System Manager select **Routing→Locations** and then select the **New** button in the window that appears. Fill in the following information:

- **Name:** Enter in a descriptive name for the location
- **Notes:** Further descriptive information
- **Managed BW:** (*Optional*) Enter in a value so Session Manager can limit the amount of traffic to other locations
- **Avg BW per Call:** Enter in an amount that Session Manager should use on a per call basis in order to calculate total bandwidth usage.
- **Location Pattern:** Enter in an IP address pattern (10.80.123.\*) or host address for entities considered to be part of this location.

The screen below shows the information as entered for the sample configuration.

The screenshot displays the Avaya Aura System Manager 6.0 web interface. The top navigation bar includes the Avaya logo, the product name 'Avaya Aura™ System Manager 6.0', and a user status message: 'Welcome, admin Last Logged on at June 2, 2010 9:48 AM'. Below this is a red breadcrumb trail: 'Home / Routing / Locations / Location Details'. On the left is a sidebar menu with categories like Elements, Events, Groups & Roles, Licenses, Routing (selected), Domains, Locations (highlighted), Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, Defaults, Security, System Manager Data, and Users. The main content area is titled 'Location Details' and contains a 'General' tab. The 'General' tab has the following fields: 'Name' (required, value: Branch\_Location\_1), 'Notes' (value: BSM1), 'Managed Bandwidth' (value: empty, unit: Kbit/sec), and 'Average Bandwidth per Call' (required, value: 80, unit: Kbit/sec). Below these is the 'Location Pattern' section, which includes an 'Add' button, a 'Remove' button, and a table with one item. The table has columns for 'IP Address Pattern' and 'Notes'. The first row shows a checkbox, a required field with the value '10.80.112.\*', and an empty 'Notes' field. At the bottom of the 'Location Pattern' section is a 'Select' dropdown with options 'All' and 'None'. The page concludes with a red asterisk indicating 'Input Required' and 'Commit' and 'Cancel' buttons.

**AVAYA** Avaya Aura™ System Manager 6.0 Welcome, admin Last Logged on at June 2, 2010 9:48 AM  
Help | About | Change Password | Log off

Home / Routing / Locations / Location Details

**Location Details** [Commit] [Cancel]

**General**

\* Name: Branch\_Location\_1  
Notes: BSM1

Managed Bandwidth: [ ] Kbit/sec  
\* Average Bandwidth per Call: 80 Kbit/sec

**Location Pattern**

[Add] [Remove]

1 Item | Refresh Filter: Enable

	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.80.112.*	

Select : All, None

\* Input Required [Commit] [Cancel]

### 6.3. Administer the Survivable Remote Session Manager as a SIP Entity

The Survivable Remote Session Manager must be added as a SIP Entity in System Manager. Navigate to **Routing** → **SIP Entities** and select the **New** button. Enter in the following information:

- **Name** A descriptive name
- **FQDN or IP Addr** Hostname or IP address of the Asset interface.
- **Type** ‘Session Manager’
- **Notes** Free-form text
- **Location** Appropriate location created in **Section 6.2**
- **Outbound Proxy** Leave blank
- **Time Zone** Time zone value appropriate for the physical location
- **Sip Link Mon** Usually set to ‘Use Session Manager Configuration’, though it can be customized on a per-entity basis

(The remaining fields on this screen will be filled out in the next two sections)

The screen below shows the information as entered for the sample configuration.

The screenshot displays the Avaya Aura™ System Manager web interface. The top navigation bar includes the Avaya logo, the text 'Avaya Aura™ System Manager', a user welcome message 'Welcome, admin Last Logged on at June 2, 2010 9:48 AM', and links for 'Help | About | Change Password | Log of'. Below the navigation bar is a red breadcrumb trail: 'Home / Routing / SIP Entities / SIP Entity Details'. On the left is a sidebar menu with categories: Elements, Events, Groups & Roles, Licenses, Routing (expanded), Domains, Locations, Adaptations, SIP Entities (highlighted), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, Defaults, Security, System Manager Data, and Users. The main content area is titled 'SIP Entity Details' and has 'Commit' and 'Cancel' buttons. It is divided into two sections: 'General' and 'SIP Link Monitoring'. The 'General' section contains fields for: Name (BSM1), FQDN or IP Address (10.80.112.15), Type (Session Manager), Notes (Branch SM S8300D), Location (Branch\_Location\_1), Outbound Proxy, Time Zone (America/Denver), and Credential name. The 'SIP Link Monitoring' section contains a single field: SIP Link Monitoring (Use Session Manager Configuration).

**AVAYA** Avaya Aura™ System Manager Welcome, **admin** Last Logged on at June 2, 2010 9:48 AM Help | About | Change Password | Log of

Home / Routing / SIP Entities / SIP Entity Details

**SIP Entity Details** [Commit] [Cancel]

**General**

\* Name: BSM1

\* FQDN or IP Address: 10.80.112.15

Type: Session Manager

Notes: Branch SM S8300D

Location: Branch\_Location\_1

Outbound Proxy:

Time Zone: America/Denver

Credential name:

**SIP Link Monitoring**

SIP Link Monitoring: Use Session Manager Configuration

## 6.4. Define Ports & Protocols for use by Survivable Remote Session Manager

To verify the port & protocol used between the core instance of Session Manager and Communication Manager, in the left pane select **Routing**→**Entity Links**.

The screen below shows that port 5060 and the TCP protocol are being used.

► Elements

► Events

► Groups & Roles

Licenses

► Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Entity Links

Edit

New

Duplicate

Delete

More Actions ▾

Commit

12 Items

Refresh

Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
<input type="checkbox"/>	<a href="#">ASM1_CM1-135.8.19.121_5060_TCP</a>	SM1	TCP	5060	Avaya-CM	5060	<input checked="" type="checkbox"/>	<a href="#">Edit</a>
<input type="checkbox"/>	<a href="#">ASM1-CS1000E</a>	SM1	TCP	5060	CS1000E-West	5060	<input checked="" type="checkbox"/>	<a href="#">Edit</a>
<input type="checkbox"/>	<a href="#">ASM1_OCS1-135.8.19.139_5070_TCP</a>	SM1	TCP	5070	Microsoft-OCS-Mediation-Server	5070	<input checked="" type="checkbox"/>	<a href="#">Edit</a>
<input type="checkbox"/>	<a href="#">BSM1 to CM-Evolution</a>	BSM1	TCP	5060	S8800-CM 6.0 ES	5060	<input checked="" type="checkbox"/>	<a href="#">Edit</a>
<input type="checkbox"/>	<a href="#">S8800-CM 6.0</a>	SM1	TCP	5060	S8800-CM 6.0 ES	5060	<input checked="" type="checkbox"/>	<a href="#">Edit</a>

In the sample configuration, TCP port 5060 is used between the core Communication Manager and Session Manager, therefore the Survivable Remote Session Manager must be configured to use this port as well. In the same screen as mentioned in the previous section, scroll down to the section titled **Entity Links** and select **Add**.

The screen below shows the information as entered for the sample configuration. Be sure to select a **Default Domain** as shown below.

Port
Add
Remove

1 Item | Refresh
Filter: Enable

<input type="checkbox"/>	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	5060	TCP	avaya.com	SIP Signaling to LSP

Select : All, None

\* Input Required
Commit
Cancel

## 6.5. Administer Entity Links

Generally a SIP trunk between a Session Manager and a telephony/messaging system is described by an Entity Link. For the Survivable Remote Session Manager, links are administered but not truly needed until some sort of outage occurs that requires the Survivable Remote Communication Manager and/or Session Manager to go into an ‘active’ mode.

To add an Entity Link, select **Entity Links** on the left panel menu and click on the **New** button (not shown). Fill in the following fields in the new row that is displayed.

- **Name** An informative name
- **SIP Entity 1** Select an instance of Session Manager
- **Protocol** Transport protocol to be used to send SIP requests
- **Port** Port number to which the other system sends its SIP requests
- **SIP Entity 2** The other SIP Entity for this link
- **Port** Port number to which the other system expects to receive SIP requests
- **Trusted** Whether to trust the other system

Click **Commit** to save changes. The following screen shows the Entity Link used in the sample network.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* BSM1 to CM-Evoluti	* BSM1	TCP	* 5060	* S8800-CM 6.0 ES	* 5060	<input checked="" type="checkbox"/>	

## 6.6. Define Survivable Remote Session Manager to System Manager

To complete the linkage between System Manager and the Survivable Remote Session Manager it's necessary to identify the SIP Entity created in the previous section as an instance of a Branch Session Manager.

As shown below, expand the **Elements** menu on the left pane then select **Session Manager** then **Session Manager Administration**. Scroll down to the section titled “**Branch Session Manager Instances**” and select **New** (not shown), and fill in the fields as described below and shown in the following screen:

Under *General*:

- **SIP Entity Name:** Select the Session Manager SIP Entity added in **Section 6.3**
- **Description:** Descriptive comment (optional)
- **Management Access Point Host Name/IP:** Enter the IP address of the Session Manager management interface (not the SIP Entity interface address)
- **Main CM for LSP:** Select the core Communication Manager instance from the drop-down
- **Direct Routing To Endpoints:** Select '**Enable**' from the drop-down
- **Adaptation for Trunk Gateway:** Select the adaptation used by the core Communication Manager. For the sample configuration no adaptation was used

Under *Security Module*:

- **Network Mask:** Enter the network mask corresponding to the IP address of Session Manager
- **Default Gateway:** Enter the IP address of the default gateway for Session Manager

All other fields can be left at their defaults.

**Edit Branch Session Manager** Comm

General | Security Module | Monitoring | Personal Profile Manager (PPM) - Connection Settings | Event Server |  
Expand All | Collapse All

**General**

SIP Entity Name

Description

\*Management Access Point Host Name/IP

\*Main CM for LSP  Refresh [View/Add CM Sy...](#)

\*Direct Routing to Endpoints

Adaptation for Trunk Gateway

**Security Module**

SIP Entity IP Address

\*Network Mask

\*Default Gateway

\*Call Control PHB

\*QOS Priority

\*Speed & Duplex

VLAN ID

## 6.7. Administer Routing Policies and Dial Pattern

Routing policies and dial patterns direct how calls will be routed to a SIP Entity. In the sample configuration a routing policy and dial pattern for the core location should already be administered. However a dial pattern must be created for the extension range that was added to accommodate the Survivable Branch location (662xxxx).

To add a dial pattern, select **Routing → Dial Patterns** on the left-pane and click on the **New** button (not shown) on the right. Fill in the following, as shown in the screens below:

Under *General*:

- **Pattern:** '662' Dialed number or prefix
- **Min:** '7' Minimum length of dialed number.
- **Max:** '7' Maximum length of dialed number.
- **SIP Domain:** 'avaya.com' SIP domain
- **Notes:** Comment on purpose of dial pattern.

Under *Originating Locations and Routing Policies*:

Click **Add**, and then select the appropriate location (or “ALL”) and **Routing Policy** from the list.

Default values can be used for the remaining fields. Click **Commit** to save the dial pattern.

The following screenshot shows the dial pattern for routing calls to Communication Manager Evolution Server.

Avaya Aura™ System Manager 6.0

Welcome, **admin** Last Logged on at June 7, 2010 2:35 PM

[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

Home / Routing / Dial Patterns / Dial Pattern Details

**Dial Pattern Details** Commit Cancel

**General**

\* **Pattern:** 662

\* **Min:** 7

\* **Max:** 7

**Emergency Call:** ☐

**SIP Domain:** avaya.com

**Notes:** to Branch location

**Originating Locations and Routing Policies**

Add Remove

1 Item | [Refresh](#) Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination
<input type="checkbox"/>	-ALL-	Any Locations	to S8800 Evolution Westminster	0	<input type="checkbox"/>	S8800-CM 6.0 ES

**NOTE:** It may seem a bit confusing to route calls to 662xxx to the ‘core’ instance of Communication Manager. However consider that under normal operation, the Survivable Remote Branch is merely a gateway controlled by the ‘core’ so all calls to the branch are actually routed to the Communication Manager Evolution Server.

## 6.8. Administer SIP Users and Survivable Branch Stations

### 6.8.1. Add a SIP User and Corresponding Station

Starting with release 5.2 it is recommended to use System Manager to add SIP users and the corresponding 96xx SIP stations on Communication Manager.

To begin entering user information, from the left pane navigate to:  
**Users→Manage Users** and select **New** (not shown)

Step 1: Enter values for the following required attributes for a new SIP user in the **General** section of the new user form.

- **Last Name:** Enter last name of user
- **First Name:** Enter first name of user

**AVAYA** Avaya Aura™ System Manager 6.0

Welcome, **admin** Last Logged on at June 4, 2010 2:28 PM  
[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

[Home](#) / [Users](#) / [Manage Users](#) / [New User](#)

**New User Profile** [Commit](#) [Cancel](#)

[General](#) | [Identity](#) | [Communication Profile](#) | [Roles](#) | [Group Membership](#) | [Default Contact List](#) | [Private Contacts](#) | [Expand All](#) | [Collapse All](#)

**General** ▾

\* **Last Name:**

\* **First Name:**

**Middle Name:**

**Description:**

[Manage Users](#)  
[Public Contact Lists](#)  
[Shared Addresses](#)  
[System Presence ACLs](#)  
[Help](#)

Step 2: Enter values for the following required attributes in the **Identity** section.

- **Login Name:** Enter extension xxxxxxxx@sip domain defined in **Section 5.4**. This field is the primary handle of the user
- **Authentication Type:** Select **Basic**
- **SMGR Login Password:** Enter an alphanumeric password which will be used to log into the System Manager application
- **Confirm Password:** Repeat value entered above
- **Shared Comm. Profile Pass.:** Enter a numeric value which will be used by the SIP phone to log in to Session Manager.
- **Confirm Password:** Repeat numeric password

---

**Identity** ▼

\* **Login Name:**

\* **Authentication Type:**

**SMGR Login Password:**

\* **Password:**

\* **Confirm Password:**

**Shared Communication Profile Password:**

**Confirm Password:**

**Localized Display Name:**


**Endpoint Display Name:**

**Honorific:**

**Language Preference:**

**Time Zone:**

---


**Step 3:** Scroll down to the **Communication Profile** section and expand the view by selecting the  icon. There should be at least one profile called **Primary** which is already defined as the default.

Under **Communication Address** select **New** to define a **Communication Address** for the new SIP user. Enter values for the following required attributes:

- **Type:** Select '**Avaya SIP**'
- **Fully Qualified Address:** Enter extension number
- **@:** Enter SIP domain defined in **Section 5.4**

Once the above information is entered select **Add** to create the new Communication Address.

**Communication Profile** ▼

Name
 Primary

Select : None

\* Name:

Default : ☒

---

**Communication Address** ▼

	Type	Handle	Domain
No Records found			

Type:  ▼

\* Fully Qualified Address:  @  ▼

The screen below shows the completed information after adding a new Communication Address.

**Communication Address** ▼

	Type	Handle	Domain
<input type="checkbox"/>	Avaya SIP	6624002	avaya.com

Select : All, None

Step 4: Scroll down to the **Session Manager Profile** section and expand the view by selecting the ► icon. Enter values for the following required attributes:

- **Primary Session Manager** Select the core Session Manager SIP entity from the drop-down
- **Origination Application Sequence** Select the application sequence defined for the Communication Manager Evolution Server
- **Termination Application Sequence** Select the application sequence defined for the Communication Manager Evolution Server
- **Survivability Server** Select the Survivable Remote Session Manager entity defined in **Section 6.3** from the drop-down
- **Home Location** Select the location defined in **Section 6.2** from the drop-down

✓ Session Manager Profile ▼

\* Primary Session Manager

SM1 ▼

Primary	Secondary	Maximum
25	0	25

Secondary Session Manager

(None) ▼

Primary	Secondary	Maximum

Origination Application Sequence

Evolution-App-Sequence ▼

Termination Application Sequence

Evolution-App-Sequence ▼

Survivability Server

BSM1 ▼

supports 3 Communication Profile (s).

\* Home Location

Branch\_Location\_1 ▼

Step 5: Scroll down to the **Endpoint Profile** section and expand the view by selecting the icon. Enter values for the following required attributes of the **Endpoint Profile** section:

- **System:** Select the instance of the Communication Manager defined for the Evolution Server
- **Use Existing Endpoints:** Enter checkmark if station admin already exists. Else, station will automatically be created
- **Extension:** Enter extension number
- **Template:** Select template for type of SIP phone.
- **Security Code:** Enter numeric value which will be used to log on to the SIP phone  
NOTE: this field must match the value entered for the **Shared Communication Profile Password** field.
- **Port:** Select IP from the drop-down
- **Delete Endpoint on Unassign of Endpoint from User:** Enter checkmark to automatically delete station from Communication Manager when the User Profile is removed in System Manager

The screen below shows the information when adding a new SIP user to the sample configuration.

---

☐ **Endpoint Profile**

\* **System**

S8800-CM6-West-Evolution

Use Existing Endpoints

☐

\* **Extension**

6624002

Endpoint Editor

\* **Template**

DEFAULT\_9630SIP\_CM\_6\_0

Set Type

9630SIP

Security Code

••••••

\* **Port**

IP

Voice Mail Number

Delete Endpoint on Unassign of Endpoint from User

☒

Step 6: While not mandatory for creating a SIP user and corresponding station on Communication Manager, it is at this point in the creation of a SIP user that it is also possible to administer Communication Manager station features, such as additional feature buttons, using System Manager. Select the **Endpoint Editor** button shown above to begin station editing. **Section 6.8.2** discusses the screens shown in the Endpoint Editor.

## 6.8.2. Add a non-SIP Station

System Manager allows for the creation of non-SIP stations on Communication Manager. Similar to Step 6 in **Section 6.7.1**, use the Endpoint Editor to create the H.323 station shown in the sample configuration (x662-4011).

**Step 1:** To begin adding a station to Communication Manager via System Manager, from the left-pane select **Elements→Endpoints→Manage Endpoints**. Next, be sure to expand the section titled **Select Devices from Communication Manager List** and select the appropriate Communication Manager instance and then select the **Show List** button as indicated below:

**AVAYA** Avaya Aura™ System Manager 6.0

Welcome, **admin** Last Logged on at June 1, 2010 2:21 PM  
[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

Home / Elements / Endpoints / Manage Endpoints

**Endpoints**

Select Device(s) from Communication Manager List ▼

3 Items | [Refresh](#) Filter: [Enable](#)

<input type="checkbox"/>	Element Name	FQDN/IP Address	Last Sync Time	Last Translation Time	Sync Type
<input type="checkbox"/>	CM-FS	10.80.100.73	June 1, 2010 2:00:53 AM - 06:00	10:00 pm MON MAY 31, 2010	Incremental
<input type="checkbox"/>	S8300D-ES	135.8.19.121	May 3, 2010 2:00:57 AM - 06:00	10:00 pm MON MAY 31, 2010	Incremental
<input checked="" type="checkbox"/>	S8800-CM6-West-Evolution	10.80.111.73	May 25, 2010 2:00:58 AM - 06:00	10:05 pm MON MAY 31, 2010	Initialization

Select : All, None

[Show List](#)

**Step 2:** Next scroll down to view the list of existing stations and select **New** to create a new station:

Show List

Endpoint List

View

Edit

New

Delete

More Actions

Advanced Search

12 Items | Refresh

Filter: Enable

<input type="checkbox"/>	Name	Extension	Port	Set Type	COS	COR	User	System
<input type="checkbox"/>	Solo, Han	6663001	S00001	9620SIP	1	1	6663001@avaya.com	CM-FS
<input type="checkbox"/>	Skywalker, Luke	6663000	S00000	9620SIP	1	1	6663000@avaya.com	CM-FS
<input type="checkbox"/>	mojo, mr	22012	S00010	9630SIP	1	1	22012@avaya.com	CM-FS
<input type="checkbox"/>	Kensington, Mrs.	22011	S00007	9630SIP	1	1	22011@avaya.com	CM-FS
<input type="checkbox"/>	Evil, Scott	22010	S00006	9630SIP	1	1	22010@avaya.com	CM-FS
<input type="checkbox"/>	Two, Number	22009	S00004	9630SIP	1	1	22009@avaya.com	CM-FS
<input type="checkbox"/>	Exposition, Basil	22008	S00012	9630	1	1	22008@avaya.com	CM-FS
<input type="checkbox"/>	Kensington, Vanessa	22007	S00008	9630SIP	1	1	22007@avaya.com	CM-FS
<input type="checkbox"/>	bench 9630 phone	22006	S00002	9630SIP	1	1	22006@avaya.com	CM-FS
<input type="checkbox"/>	h.323 video2	22003	S00029	9630	1	1		CM-FS
<input type="checkbox"/>	h.323 video1	22002	S00026	9630	1	1		CM-FS
<input type="checkbox"/>	Evil, Dr.	22001	S00023	4620	1	1		CM-FS

Select : All, None

**Step 3:** In the **Add Endpoint** screen that appears, the following fields must be administered at a minimum:

- **Template** Select the appropriate station template for the set type to be used
- **Port** Enter in the port for the station. For IP telephones this will always be 'IP'
- **Name** Enter the station user name
- **Extension** Enter in the desired extension number or choose one from the range of available extensions displayed in System Manager
- **Security Code** For IP stations, enter in a numeric password which will be used to log in to the IP telephone

**AVAYA** Avaya Aura™ System Manager 6.0

Welcome, **admin** Last Logged on at June 4, 2010 2:28 PM

Help | About | Change Password | Log off

Home / Elements / Endpoints / Manage Endpoints / Add Endpoint

**Add Endpoint**

[Commit] [Schedule] [Clear] [Cancel]

[Save As Template]

\* System: S8800-CM6-West-Evolut

\* Extension: 6624011

\* Template: DEFAULT\_1616\_CM\_6\_0

\* Set Type: 1616

\* Port: IP

\* Security Code: .....

Name: Natalie Portman

General Options | Feature Options | Site Data | Abbreviated Call Dialing | Enhanced Call Fwd | Button Assignment | Group Membership

Expand All | Collapse All

**General Options**

\* Class of Restriction (COR): 1

\* Class Of Service (COS): 1

\* Emergency Location Ext: 6624011

\* Message Lamp Ext.: 6624011

\* Tenant Number: 1

Native Name:

Coverage Path 1:

Coverage Path 2:

Lock Message: ☐

Step 4: Scroll down to see the remaining sections and fields that can be configured for a station. The screenshots below are an example of some of the additional station administration.

Select **Commit** to add the station to Communication Manager immediately or **Schedule** to add the station at a later time.

General Options | Feature Options | Site Data | Abbreviated Call Dialing | Enhanced Call Fwd | Button Assignment | Group Membership |  
Expand All | Collapse All

**General Options**

* Class of Restriction (COR)	<input type="text" value="1"/>	* Class Of Service (COS)	<input type="text" value="1"/>
* Emergency Location Ext	<input type="text" value="6624011"/>	* Message Lamp Ext.	<input type="text" value="6624011"/>
* Tenant Number	<input type="text" value="1"/>	Native Name	<input type="text"/>
Coverage Path 1	<input type="text"/>	Coverage Path 2	<input type="text"/>
Lock Message	<input type="checkbox"/>		

**Feature Options**

Active Station Ringing	<input type="text" value="single"/>	Multimedia Mode	<input type="text" value="enhanced"/>
Auto Answer	<input type="text" value="none"/>	MWI Served User Type	<input type="text" value="Select"/>
Coverage After Forwarding	<input type="text" value="system"/>	Per Station CPN - Send Calling Number	<input type="text" value="Select"/>
Display Language	<input type="text" value="english"/>	Personalized Ringing Pattern	<input type="text" value="1"/>
Hunt-to Station	<input type="text"/>	Time of Day Lock Table	<input type="text" value="Select"/>
Remote Soft Phone Emergency Calls	<input type="text" value="as-on-local"/>	Service Link Mode	<input type="text" value="as-needed"/>
Loss Group	<input type="text" value="19"/>	Speakerphone	<input type="text" value="2-way"/>
LWC Reception	<input type="text" value="spe"/>	Survivable COR	<input type="text" value="internal"/>
Survivable GK Node Name	<input type="text" value="Q"/>	EC500 State	<input type="text" value="enabled"/>
Media Complex Ext	<input type="text"/>	AUDIX Name	<input type="text" value="Select"/>
Call Appearance Display Format	<input type="text" value="disp-param-default"/>	IP Phone Group ID	<input type="text"/>
Prime Appearance Preference	<input type="text"/>	Voice Mail Number	<input type="text"/>
Location	<input type="text"/>		

**Features**

<input type="checkbox"/> Always Use	<input type="checkbox"/> H.320 Conversion
<input type="checkbox"/> Audible Message Waiting	<input type="checkbox"/> Idle Appearance Preference
<input type="checkbox"/> Auto Select Any Idle Appearance	<input type="checkbox"/> IP Audio Hairpinning
<input type="checkbox"/> Bridged Call Alerting	<input type="checkbox"/> IP SoftPhone
<input type="checkbox"/> Bridged Idle Line Preference	<input checked="" type="checkbox"/> LWC Activation
<input type="checkbox"/> CDR Privacy	<input type="checkbox"/> LWC Log External Calls
<input type="checkbox"/> Conf/Trans On Primary Appearance	<input type="checkbox"/> Multimedia Early Answer
<input checked="" type="checkbox"/> Coverage Message Retrieval	<input checked="" type="checkbox"/> Mute Button Enabled
<input type="checkbox"/> IP Video	<input type="checkbox"/> Per Button Ring Control
<input type="checkbox"/> Data Restriction	<input checked="" type="checkbox"/> Precedence Call Waiting
<input checked="" type="checkbox"/> Direct IP-IP Audio Connections	<input checked="" type="checkbox"/> Redirect Notification
<input type="checkbox"/> Display Client Redirection	<input checked="" type="checkbox"/> Restrict Last Appearance
<input type="checkbox"/> Select Last Used Appearance	<input type="checkbox"/> EMU Login Allowed
<input checked="" type="checkbox"/> Survivable Trunk Dest	<input type="checkbox"/> Bridged Appearance Origination Restriction

Site Data ▶
Abbreviated Call Dialing ▶
Enhanced Call Fwd ▶
Button Assignment ▶
Group Membership ▶
*Required
<input type="button" value="Commit"/> <input type="button" value="Schedule"/> <input type="button" value="Clear"/> <input type="button" value="Cancel"/>

## 6.9. Synchronize Communication Manager with System Manager

Any time changes are made to Communication Manager outside of the System Manager interface, it is recommended to perform an incremental synchronization between the two to ensure they have identical configurations.

Select **Elements → Inventory → Manage Elements → Synchronization → Communication System** on the left. Check the appropriate **Element Name**, click **Incremental Sync data for selected devices** and click **Now**. This may take some time to complete while System Manager examines the recent changes to the configuration on Communication Manager.

## 7. Configure the Avaya one-X® Deskphone Edition for 9600 SIP IP Telephone

Before configuring the 9600 Series SIP telephone please refer to the reference documents in **Section 11** for a more complete explanation on setting up these telephones. Also it is important to realize that the 9600 Series phones support both H.323 and SIP firmware, so be sure that the phone is running with SIP firmware before proceeding.

At a minimum, the following parameters must be set for the phone to successfully register with both instances of Session Manager:

- IP address, subnet mask, default gateway of the phone itself.
- SIP domain
- SIP Proxy Server Addresses (in this case: Session Manager & Survivable Remote Session Manager)
- Username (usually the extension number like 662-4000)
- Password

All but the last two values can be configured with a combination of DHCP scopes and the **46xxsettings.txt** file or by manually programming these values directly on the phone itself.

The following screens illustrate how to set these values manually on the phone itself via the keypad. See the references in **Section 11** on how to configure DHCP and a 46xxsettings.txt file to automate the procedure described below.

### 7.1. Configuration Using DHCP and 46xxsettings.txt

This section discusses the basic settings used in the sample configuration that can be used in the DHCP scope and 46xxsettings.txt file in order to configure the above parameters. There are a significant number of options one can configure via DHCP and the 46xxsettings.txt file. For additional information on this topic see reference [9] in **Section 11**.

#### 7.1.1. DHCP Settings

In the sample configuration, a DHCP server was configured at the branch location to supply IP telephones with an IP address, subnet mask and default gateway. In addition an Option 242 scope was created to assign the following values:

Parameter Name & Value	Description
MCIPADD=10.80.111.76,10.80.111.73,10.80.112.12	IP address of a CLAN, Procr and LSP interface for H.323 IP phones to register to Communication Manager.
MCPORT=1719	Port for H.323 IP phones to use during registration.
HTTPSRVR=10.80.112.13	IP address(es) or DNS name(s) of HTTP file server(s) used by all IP phones for file download (46xxsettings.txt file, language files, code) during startup.

### 7.1.2. 46xxsettings.txt Parameters

In addition to receiving basic settings via DHCP (IP Address, subnet mask, default gateway & HTTP server), Avaya IP telephones can be automatically configured with additional settings by downloading a 46xxsettings.txt file from an HTTP/HTTPS server. In the sample configuration only a small subset of these parameters were used to enable basic functionality and survivability.

The following parameters were used in the 46xxsettings.txt file:

Parameter Name & Value	Description
SET SIPDOMAIN "avaya.com"	Sets the SIP domain name to be used during registration.
SET SIMULTANEOUS_REGISTRATIONS 2	The number of Session Managers in the configuration that the phone will simultaneously register with.
SIP_MODE 0	Defines the SIP operational mode. If set to 0 then SIP Proxy/Registrar is used. If set to 1 then SIP Proxy/Registrar will not be used and phone will operate in peer-to-peer mode
SET ENABLE_G711U 1	Enables the phone to communicate using the G.711U-law codec.
SET ENABLE_G729 1	Enables the phone to communicate using the G.729(A) codec.
SET DISPLAY_NAME_NUMBER 1	Provides display of name and number of incoming call. -If set to 0 then phone will display only the number of the incoming call. -If set to 1 then the phone will display the name and number of incoming call.
SET SIP_CONTROLLER_LIST 10.80.100.28:5060;transport=tcp,10.80.112.15:5060 ;transport=tcp	Provides the ability to configure a list of SIP proxies/registrars. The list may contain one or more comma separated controllers where a controller has the following format: host[:port][;transport=xxx] host is an IP address in dotted-decimal format or DNS name. [:port] is the optional port number. [:transport=xxx] is the optional transport type where xxx can be tls, tcp, or udp. - If a port number is not specified the default value of 5060 for TCP and UDP or 5061 for TLS is used. -If a transport type is not specified the default value of tls is used.
SET ENABLE_PPM_SOURCED_SIPPROXYSRVR 1	Enables PPM as a source of SIP Proxy server information. When this is set to 1 then proxy server information discovered via PPM will be used even if the initial values are supplied via DHCP.
SET FAILBACK_POLICY auto	When this parameter is set to "auto", the phone's active controller will always be the highest priority available controller. If FAILBACK_POLICY parameter is set to "admin", then a controller lower down the priority list may be active.
SET SIPREGPROXYPOLICY simultaneous	If this parameter is "alternate" and a user is logged-in, the phone will attempt and maintain a single active SIP registration with the highest priority controller. If this parameter is "simultaneous" and a user is logged-in, the phone will attempt and maintain active SIP registrations with all available controller(s).

SET DISCOVER_AVAYA_ENVIRONMENT 1	If the DISCOVER_AVAYA_ENVIRONMENT parameter value is 1, the phone discovers (determines) if the controller supports the Advanced SIP Telephony (AST) feature set or not. The phone will send a SUBSCRIBE request to the active controller for the Feature Status Event Package (avaya-cm-feature-status). If the request succeeds, then the phone proceeds with PPM Synchronization. If the request is rejected, is proxied back to the phone or does not receive a response, the phone will assume that AST features are not available. If the parameter value is 0, the phone operates in a mode where AST features are not available.
----------------------------------	--

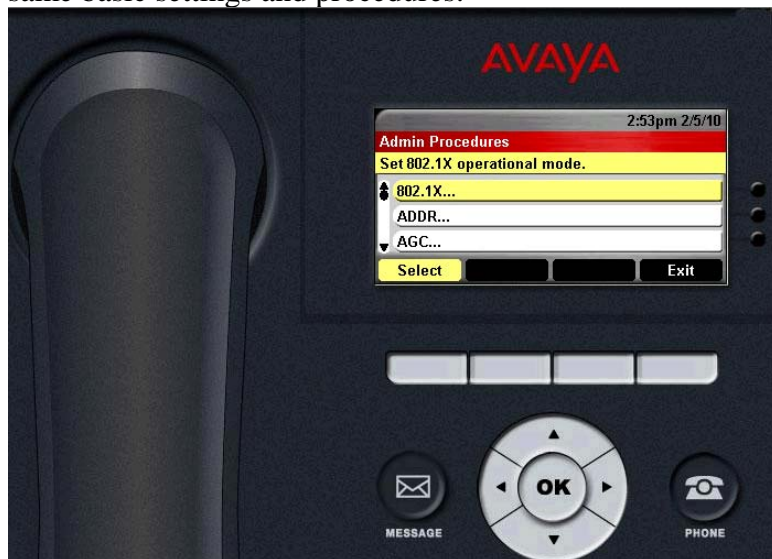
## 7.2. Configure the Avaya one-X® Deskphone Edition for 9600 SIP IP Telephone Manually

### 7.2.1. Configure IP Address, Subnet Mask & Default Gateway

To access the 9600 Series telephone setup screens shown below press the following keys on the keypad:

**mute-c-r-a-f-t** # (mute-2-7-2-3-8-#). The screen shown below will appear on the phone.

NOTE: These screenshots are from a 9650C telephone though all 9600 Series phones use the same basic settings and procedures:

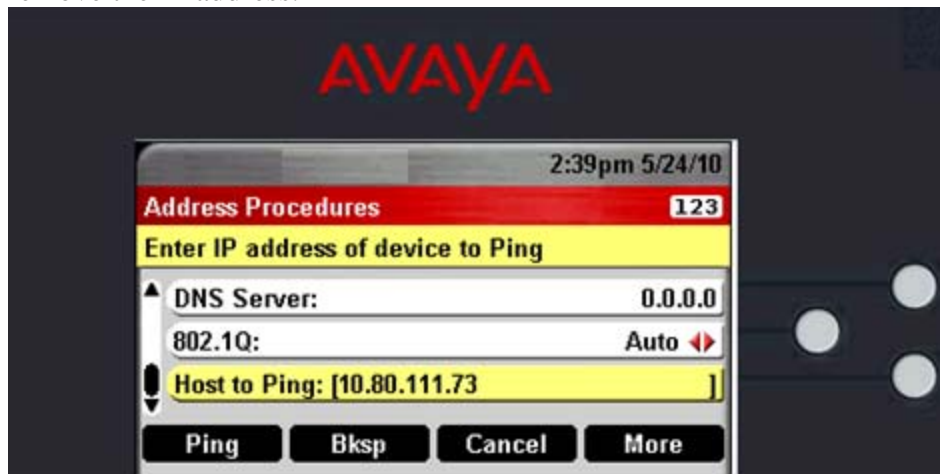


Using the phone's down arrow, scroll down one row and select **ADDR...**. The following screen appears:

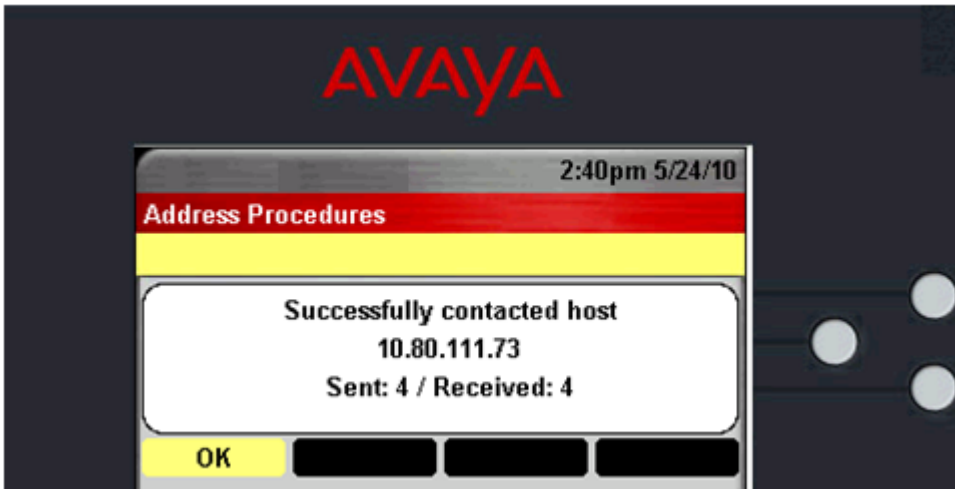


Using the up and down scroll buttons, select the appropriate fields for editing, pressing the **Change** button to edit each field. Scroll down further to see the fields for **Mask** (subnet mask), **HTTPS & HTTP File Server**, **DNS Server**, **802.1Q**, **VLAN ID**, and **VLAN Test**.

The last row on this screen is **Host To Ping**. If needed, enter in an IP address and press the **PING** key to test network connectivity. Press the **Bksp** button when the test is complete to remove the IP address.



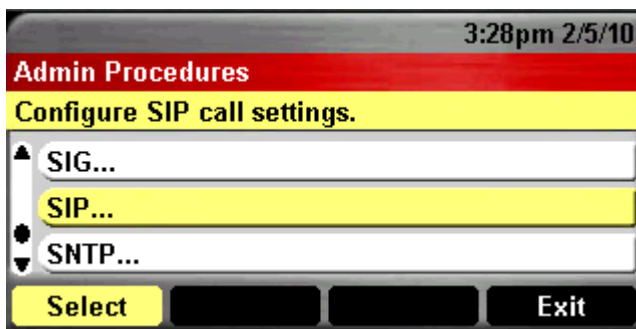
Shown below is a screenshot of a successful test to 10.80.120.28:



Once programming is completed on the above screens be sure to press **Save** to get back to the main screen and save the configuration.

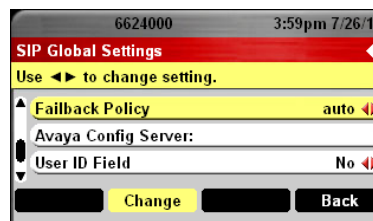
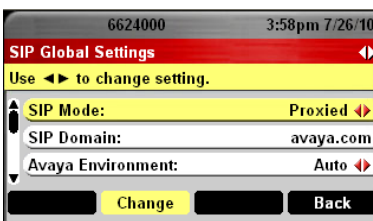
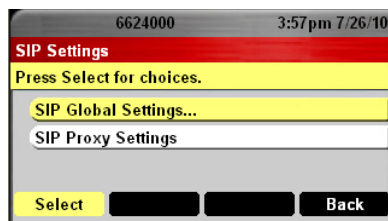
### 7.2.2. Configure SIP Global and Proxy Settings

The next steps are to configure the SIP Domain and the SIP Proxy server addresses. From the main admin screen, scroll down and select **SIP...**

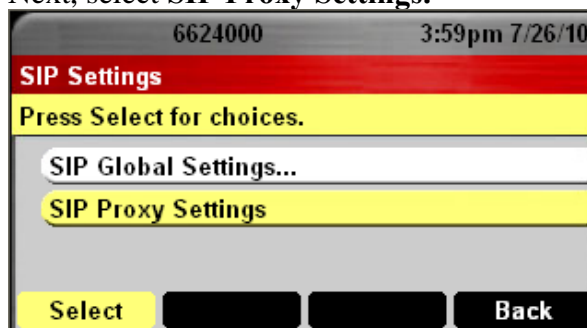


In the screen that appears select **SIP Global Settings**, The options as shown in the image below will appear. Verify the following are set:

- **Sip Mode**                      **Proxied**
- **SIP Domain**                      **avaya.com**
- **Avaya Environment**              **Auto**
- **Registration Policy**              **simultaneous** to support registration to the core and survivable instances of Session Manager
- **Failback Policy**                      **auto**
- **User ID field**                      **no**

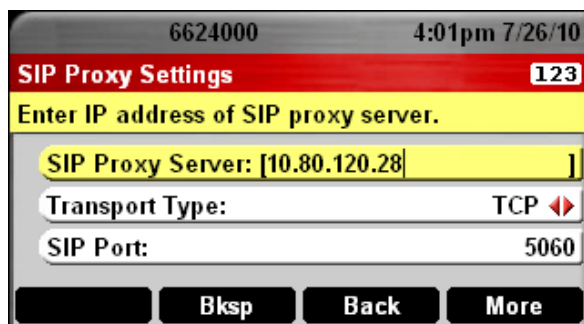


Select the **Save** button when complete.  
Next, select **SIP Proxy Settings**.



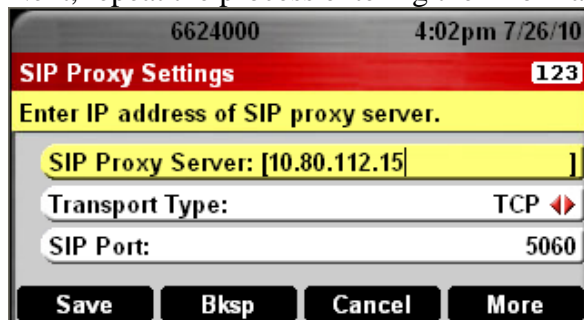
Select **NEW** and the following screen appears. Enter the following information for the core instance of Session Manager.

- **SIP Proxy Server**      Address of Session Manager SIP Entity interface
- **Transport Type**      TCP (can be TLS or UDP as well)
- **SIP Port**              5060 for TCP & UDP, 5061 for TLS



Select **Save** when complete.

Next, repeat the process entering the information for the Survivable Remote Session Manager.



Select **Save** when complete.

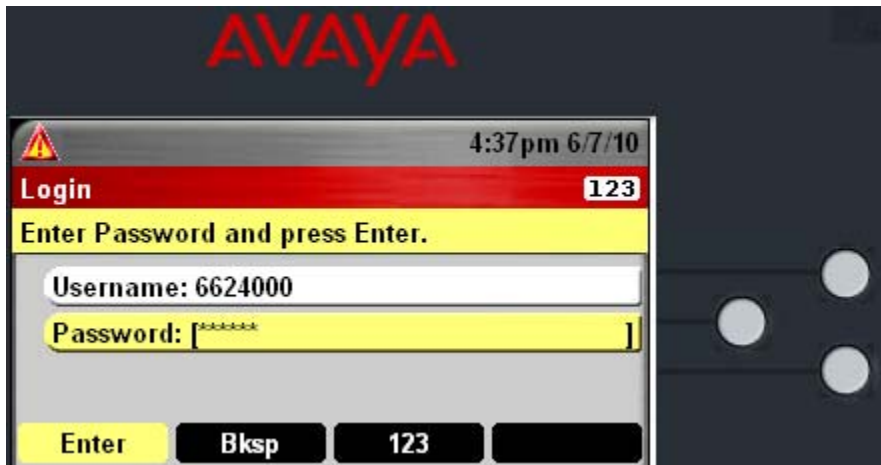
Select **Back** two times to get back to the main menu.

Select **Exit** to complete the configuration. The phone will reboot.

### 7.2.3. Log in Phone to Avaya Aura™ Session Manager

Once the phone has rebooted, a login screen will be presented. Enter the following information:

- **Username** Extension number/User created in **Section 6.8.2**
- **Password** Use the Security Code as it was programmed when creating a SIP user in **Section 6.8.2**



Select Enter and the phone will log in to Session Manager immediately. Shown below is a successfully logged in 9650C phone:



## 8. Verify Installation

This section will show the various steps and administration screens to access to ensure that Avaya Aura for Survivable Remote has been properly administered, is registered, and is ready to go active in an outage scenario.

### 8.1. Verify Avaya Aura™ Communication Manager Evolution Server

#### 8.1.1. Verify Survivable Server Status

Open a SAT session on the Communication Manager Evolution Server.

Use the command **list survivable-processor** to verify that the Survivable Remote Communication Manager is registered and has a current copy of the translations:

list survivable-processor						
SURVIVABLE PROCESSORS						
Record Number	Name/ IP Address	Type	Reg	Act	Translations Updated	Net Rgn
1	BSM-LSP1 10.80.112.12 No V6 Entry	LSP	y	n	22:05 6/07/2010	3

#### 8.1.2. Verify Media Gateway Registration Status

Use the command 'list media-gateway' to verify that the branch gateway is registered with Communication Evolution Server.

```
list media-gateway
```

MEDIA-GATEWAY REPORT						
Num	Name	Serial No/ FW Ver/HW Vint/ RecRule	IPV4 Address/ IPV6 Address/ Cntrl IP Addr	Type	NetRgn	Reg?
1	G450 BSM1	08IS35197397 30 .12 .1 /1 1	10.80.112.9 10.80.111.76	g450	3	y

### 8.2. Verify Avaya Aura™ Session Manager

#### 8.2.1. Verify Database Replication Status

Log in to System Manager. Navigate to **System Manager Data→Replication** on the left-pane. In the screen that appears select the checkbox next to the replica group called **SessionManagers** (not shown). Select the button called **View Replica Nodes** (not shown). The following screen indicates all instances of Session Manager known to System Manager are properly synchronized.

- Elements
- Events
- Groups & Roles
- Licenses
- Routing
- Security
- System Manager Data
  - Backup and Restore
  - Data Retention
  - Extension Packs
  - Replication
  - Scheduler
  - Settings
  - Users

## Replica Nodes

Replica Nodes

[View Details](#)
[Repair](#)
[Remove](#)
[Show All Replica Groups](#)

3 Items | [Refresh](#) Filter: [Enable](#)

<input type="checkbox"/>	Replica Node Host Name	Product	Synchronization Status	Last Synchronization Time
<input type="checkbox"/>	asm1.interop.avaya.com		Synchronized	June 7, 2010 4:57:22 PM -06:00
<input type="checkbox"/>	asm2.interop.avaya.com		Synchronized	June 7, 2010 4:57:16 PM -06:00
<input type="checkbox"/>	BSM1-SM1.avaya.com		Synchronized	June 7, 2010 4:56:27 PM -06:00

Select : [All](#), [None](#)

### 8.2.2. Verify Status of 9600 Series SIP Telephones

Log in to System Manager. Navigate to **Elements**→**Session Manager**→**System Status**→**User Registrations** on the left-pane to verify that branch endpoints are registered to the core instance of Session Manager as well as the Survivable Remote Session Manager.

As shown below from the sample configuration, extension 6624001, an extension at the branch, is registered to both instances. Extension 6664401, an extension at the ‘core’ is registered only to the ‘core’ (or primary) instance of Session Manager.

11 Items Found   <a href="#">Refresh</a>   Show <a href="#">ALL</a>							Filter: <a href="#">Disable</a> , <a href="#">Apply</a> , <a href="#">Clear</a>		
<input type="checkbox"/>	Address	Login Name	First Name	Last Name	Location	IP Address	Registered		
							Prim	Sec	Surv
<input type="checkbox"/>	662*								
<input type="checkbox"/>	6624001@avaya.com	6624001@avaya.com	Michael	Corleone	Branch_Location_1	10.80.112.30:5061	<input checked="" type="checkbox"/> (AC)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	6663000@avaya.com	6663000@avaya.com	Luke	Skywalker	Location 1 Subnet 10.80.100.x	10.80.100.39	<input checked="" type="checkbox"/> (AC)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	6663001@avaya.com	6663001@avaya.com	Han	Solo	Location 1 Subnet 10.80.100.x	10.80.100.40	<input checked="" type="checkbox"/> (AC)	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	6664006@avaya.com	6664006@avaya.com	Admiral	Ackbar	Location 1 Subnet 10.80.60.x	10.80.60.226	<input checked="" type="checkbox"/> (AC)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	6664007@avaya.com	6664007@avaya.com	Padmé	Amidala	Location 1 Subnet 10.80.60.x	10.80.60.227	<input checked="" type="checkbox"/> (AC)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	6664401@avaya.com	6664401@avaya.com	Jarjar	Binks	Location 1 Subnet 10.80.100.x	10.80.100.46	<input checked="" type="checkbox"/> (AC)	<input type="checkbox"/>	<input type="checkbox"/>

## 9. Survivability Scenarios

The verification scenarios for the sample configuration described in these Application Notes included the following:

- When the Survivable Branch location loses WAN connectivity back to the ‘core’ that the Survivable Remote Session Manager and Communication Manager will go ‘active’ in the configured time-frame.
- Active calls between 9600 Series SIP telephones at the branch and the core will stay up in the event that the Survivable Remote goes ‘active’ (though the LAN/WAN connection is still active).

- Active calls between 9600 Series SIP telephones within the branch will stay up in the event that the Survivable Remote goes ‘active’ because of a LAN/WAN outage back to the core.
- During ‘sunny day’ operations 9600 Series SIP telephones show they are registered to both the core Session Manager and the Survivable Remote Session Manager.
- During ‘cloudy day’ operations 9600 Series SIP telephones show they are registered to only the Survivable Remote Session Manager.
- H.323 IP Telephones at the branch automatically re-register to the Survivable Remote Communication Manager in the event of a LAN/WAN outage.
- When a branch location in survivable mode re-registers back to the ‘core’, IP phones on active calls at the branch stay up until either side decides to hang up.
- When a branch location in survivable mode re-registers back to the ‘core’, inactive 9600 Series SIP telephones automatically re-register back to the ‘core’ Session Manager.

## 10. Conclusion

As illustrated in these Application Notes, Avaya Aura™ for Survivable Remote can be configured as a survivable solution for a branch location in the event the branch loses LAN/WAN connectivity back to the core.

## 11. References

Generally, all product documentation for Avaya products may be found at <http://support.avaya.com>. Below is a list of specific documents that should be used for reference:

### Avaya Aura™ Session Manager 6.0:

- [1] *Avaya Aura™ Session Manager Overview*, Doc ID 03-603323, available at <http://support.avaya.com>.
- [2] *Administering Avaya Aura™ Session Manager*, Doc ID 03-603324 available at <http://support.avaya.com>.
- [3] *Installing and Upgrading Avaya Aura™ Session Manager 6.0*, Doc ID 03-603324, available at <http://support.avaya.com>.
- [4] *Installing and Upgrading Avaya Aura™ System Manager 6.0*, available at <http://support.avaya.com>.
- [5] *Maintaining and Troubleshooting Avaya Aura™ Session Manager 6.0*, Doc ID 03-603325, available at <http://support.avaya.com>.

### Avaya Aura™ Communication Manager 6.0:

- [6] *Administering Avaya Aura™ Communication Manager as a Feature Server*, Doc # 03-

603479, Issue 1.2, Release 5.2 January 2010, available at <http://support.avaya.com>.

- [7] *Administering Avaya Aura™ Communication Manager*, Doc ID 03-300509, June 2010, available at <http://support.avaya.com>.
- [8] *Avaya one-X™ Deskphone Edition for 9600 Series SIP IP Telephones: Administrator Guide, Release 2.6*. Doc ID 16-601944 . July 2010. <http://support.avaya.com>
- [9] *Avaya one-X™ Deskphone Edition for 9600 Series IP Telephones Administrator Guide Release 3.1*. Doc ID 16-300698. November 2009. <http://support.avaya.com>
- [10] *Avaya Toll Fraud Security Guide*, Doc ID 555-025-600, February 2010, available at <http://support.avaya.com>

Avaya Application Notes:

- [11] *Configuring SIP Trunks Among Avaya Aura™ Session Manager 6.0, Avaya Aura™ Communication Manager Evolution Server 6.0, Avaya one-X™ Deskphone Edition for 9600 Series SIP IP Telephones, and Avaya (formerly Nortel) Communication Server 1000E 6.0*, available at <http://www.avaya.com>.
- [12] *Configuring 96xx SIP Phones with Avaya Aura™ Session Manager, 5.2 – Issue 1.0* available at <http://www.avaya.com>

---

**©2010 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Solution & Interoperability Test Lab at [interoplabnotes@list.avaya.com](mailto:interoplabnotes@list.avaya.com)